

AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions, and listings, of claims in this application:

1 1. (Currently Amended) A communications network security method comprising:
2 identifying a plurality of routes that define a first communications network;
3 identifying a plurality of hosts associated with the first communications network
4 as a function of the plurality of routes;
5 ~~performing-receiving~~ a census of the first communications network as a function
6 of the plurality of hosts to determine a topology of the first communications network;
7 probing at least one host of the plurality hosts of the first communications
8 network by transmitting a packet to the host, the host being selected from the census
9 results and the packet having at least a source address which is associated with a second
10 communications network; and
11 determining a security characteristic of the probed host as a function of a response
12 by the probed host in receiving the packet, the security characteristic being a measure of
13 connectivity between the first communications network and the second communications
14 network, the measure of connectivity being an indication of connectivity between the first
15 communications network and the second communications network.

1 2. (Previously Amended) The method of claim 1 wherein the source address is an
2 IP address associated with a host external to the first communications network, and the
3 external host being associated with the second communications network.

1 3. (Original) The method of claim 2 wherein the response of the probed host to
2 the receipt of the packet includes transmitting a second packet, the second packet being
3 derived using at least a portion of information from the received packet.

1 4. (Cancelled) .

1 5. (Cancelled.)

1 6. (Previously Amended) The method of claim 5 wherein the measure of
2 connectivity is determined by the further operation of:

3 monitoring the probed host to determine the response, and if the response includes
4 a transmission of a second packet from the probed host, generating a security alert
5 message identifying the probed host as a security risk.

1 7. (Previously Amended) The method of claim 3 wherein the first
2 communications network and the second communications network have different security
3 levels.

1 8. (Previously Amended) The method of claim 3 wherein the transmitted packet
2 is a TCP packet which returns a TCP packet in response thereto.

1 9. (Previously Amended) The method of claim 3 wherein the second packet is a
2 UDP packet or an ICMP packet, which returns either a UDP packet or ICMP packet in
3 response thereto.

1 10. (Currently Amended) A method for analyzing network security of a first
2 communications network, the method comprising:

3
4 receiving a census of the first communications network;

5 transmitting a packet from a host of a second communications network to a
6 particular one host of a plurality of hosts internal to the first communications network,
7 the internal host being selected from the census, and the packet being generated as a
8 function of both an IP address associated with the host of the second communications
9 network and an IP address associated with the internal host of the first communications
10 network; and

11 determining a security characteristic of the particular one internal host of the first
12 communications network as a function of a response by the internal host to the receipt of
13 the packet, the security characteristic being a measure of connectivity between the first

14 communications network and the second communications network, the measure of
15 connectivity being an indication of connectivity between the first communications
16 network and the second communications network.

1 11. (Previously Amended) The method of claim 10 wherein the measure of
2 connectivity is a function of whether the internal host of the first communications
3 network communicates with the host of the second communications network, and the
4 measure of connectivity being determined by the further operation of:

5 monitoring the internal host to determine the response, and if the response
6 includes a transmission of a second packet from the internal host, generating a security
7 alert message identifying the internal host as a security risk.

1 12. (Original) The method of claim 11 wherein the second packet is derived
2 using at least a portion of information from the transmitted packet.

1 13. (Cancelled).

1 14. (Previously Amended) The method of claim 12 wherein the internal host is a
2 dual-homed host.

1 15. (Previously Amended) The method of claim 11 wherein the security
2 characteristic includes an indication that the internal host is outside any security measures
3 provided by a firewall associated with the first communications network.

1 16. (Currently Amended) A communications system comprising:
2 a first plurality of computers associated with a first communications network;
3 a second plurality of computers associated with a second communications
4 network; and
5 a security host computer which determines a security characteristic of a first
6 computer from the plurality of computers, the security characteristic being a measure of
7 connectivity between the first communications network and the second communications

8 network by probing the first computer by transmitting a packet to the first computer, the
9 first computer being selected from a census of the first communications network and the
10 packet being generated as a function of both an IP address associated with a second
11 computer of the second plurality of computers and an IP address associated with the first
12 computer, and determining the measure of connectivity as a function of a response of the
13 first computer to receiving the packet, the measure of connectivity being an indication of
14 connectivity between the first communications network and the second communications
15 network.

1 17. (Original) The communications system of claim 16 wherein the security host
2 computer is associated with the first communications network.

1 18. (Previously Amended) The communications system of claim 17 wherein the
2 response of the first computer to the receipt of the packet includes transmitting a second
3 packet, the second packet being derived using at least a portion of information from the
4 received packet.

1 19. (Previously Amended) The communications system of claim 18 wherein the
2 security host computer determines the measure of connectivity by monitoring the probed
3 first computer to determine the response, and if the response includes the transmission of
4 the second packet from the probed host, generating a security alert message identifying
5 the first computer as a security risk.

1 20. (Previously Amended) The communications system of claim 17 wherein the
2 first communications network is an intranet and the second communications network is
3 an Internet, and the first communications network and the second communications
4 network have different security levels.

1 21. (Currently Amended) A security host computer comprising:

2 means for performing a census of a first communications network and
3 determining a topology of the first communications network, the topology being defined
4 by at least one computer,

5 means for probing the at least one computer by transmitting a packet to the
6 computer, the computer being selected from the census results and the packet being
7 generated as a function of the topology, an IP address associated with a particular host
8 computer associated with a second communications network and an IP address associated
9 with the computer, the second communications network being separate from the first
10 communications network; and

11 a monitor for determining a security level of the computer as a function of a
12 response by the computer to the receipt of the packet, and the security level being a
13 measure of connectivity between the first communications network and the second
14 communications network, the measure of connectivity being an indication of connectivity
15 between the first communications network and the second communications network.

1 22. (Previously Amended) The security host computer of claim 21 wherein the
2 measure of connectivity is determined by monitoring the computer's response, and if the
3 response includes a transmission of a second packet from the computer, a security alert
4 message identifying the computer as a security risk is generated.

1 23. (Previously Amended) The security host computer of claim 22 wherein the
2 first communications network and the second communications network have different
3 security levels.

1
2 24. (Currently Amended) A machine-readable medium having stored thereon a
3 plurality of instructions, the plurality of instructions including instructions that, when
4 executed by a machine, cause the machine to perform of a method for analyzing a first
5 communications network's integrity by receiving a census of the first communications
6 network; probing a host by transmitting a packet to the host, the host being selected from
7 the census results and the packet being derived as a function of a topology of the first
8 communications network and the packet having a source address which is associated with

9 a second communications network; and determining the first communications network's
10 integrity as a function of a response by the probed host in receiving the packet wherein
11 the response indicates a measure of connectivity between the first communications
12 network communicates and the second communications network, and the measure of
13 connectivity being an indication of connectivity between the first communications
14 network and the second communications network.

1 25. (Cancelled) .

1 26. (Currently Amended) The machine-readable medium of claim 25-24 wherein
2 the response of the probed host to the receipt of the packet includes transmitting a second
3 packet, the second packet being derived using at least a portion of information from the
4 received packet.

1 27. (Previously Amended) The machine-readable medium of claim 26 wherein
2 the first communications network is an intranet, and the second communications network
3 is an Internet.